HackOrbit 2025

2_Bit_Army

Theme: Artificial Intelligence and Machine Learning

Problem Statement:

The issue is that, although India handled over 10 billion UPI transactions in May 2025, totaling ₹17.3 trillion, UPI-based scams (phishing messages, fake QR codes, and fraudulent payment requests) have increased by 30% annually. Students, business owners, and senior citizens who lack the means to instantly confirm authenticity are among the victims. To identify and flag scams prior to money transfers, we require an AI-driven solution.

PROPOSED SOLUTION

The system you're describing is a comprehensive tool designed to enhance security by analyzing UPI transaction screenshots. Here's a breakdown of its functionality:

OCR Engine: This component is responsible for extracting both textual information and QR code data from uploaded screenshots of UPI transactions. It ensures that all relevant details are captured for further analysis.

NLP Classifier: Utilizing natural language processing, this classifier examines the extracted text for potential scam indicators. It looks for signs such as urgency cues, fake merchant names, and suspicious syntax that might suggest fraudulent activity.

Scam Risk Assessment: The system assigns a scam risk score ranging from 0 to 100%, indicating the likelihood of the transaction

Actionable Suggestions: Based on the risk assessment, the tool provides users with practical advice on how to proceed. Options include blocking the transaction, verifying the details, or proceeding if no risk is detected.

Modular Design: The tool is designed to be flexible and adaptable, making it suitable for deployment as a web application, a browser plugin, or a mobile widget. This modularity ensures that it can be easily integrated into various platforms and user environments.

Flow Chart of Fraud Detection

User Upload: Screenshot/Message

OCR Extraction: Text & QR Data

NLP Model: Scam vs Safe

Risk Score + Trigger Highlights

User Alert & Suggestion

When a user uploads a UPI payment screenshot or pastes a suspicious request, our OCR engine extracts readable text and QR metadata. The NLP classifier, specifically trained on genuine Indian scam patterns, analyzes urgency cues, counterfeit merchant details, and formatting inconsistencies. It provides a risk score and highlights the specific phrases or elements that influenced the evaluation, ensuring transparency and building user trust.

Dual-mode detection: works on images and text

Explainable AI: highlights specific scam phrases

Indian context: trained on local scam datasets (WhatsApp, SMS, app screenshots)

Lightweight: runs in-browser or offline on-device

Integration-ready: can plug into UPI apps or be offered as a Chrome/Android extension

Optical Character Recognition (OCR) technology faces several challenges when dealing with low-resolution or stylized screenshots. These limitations can lead to inaccuracies, such as false positives, which may undermine user trust. To mitigate this, careful threshold tuning is essential to balance sensitivity and specificity.

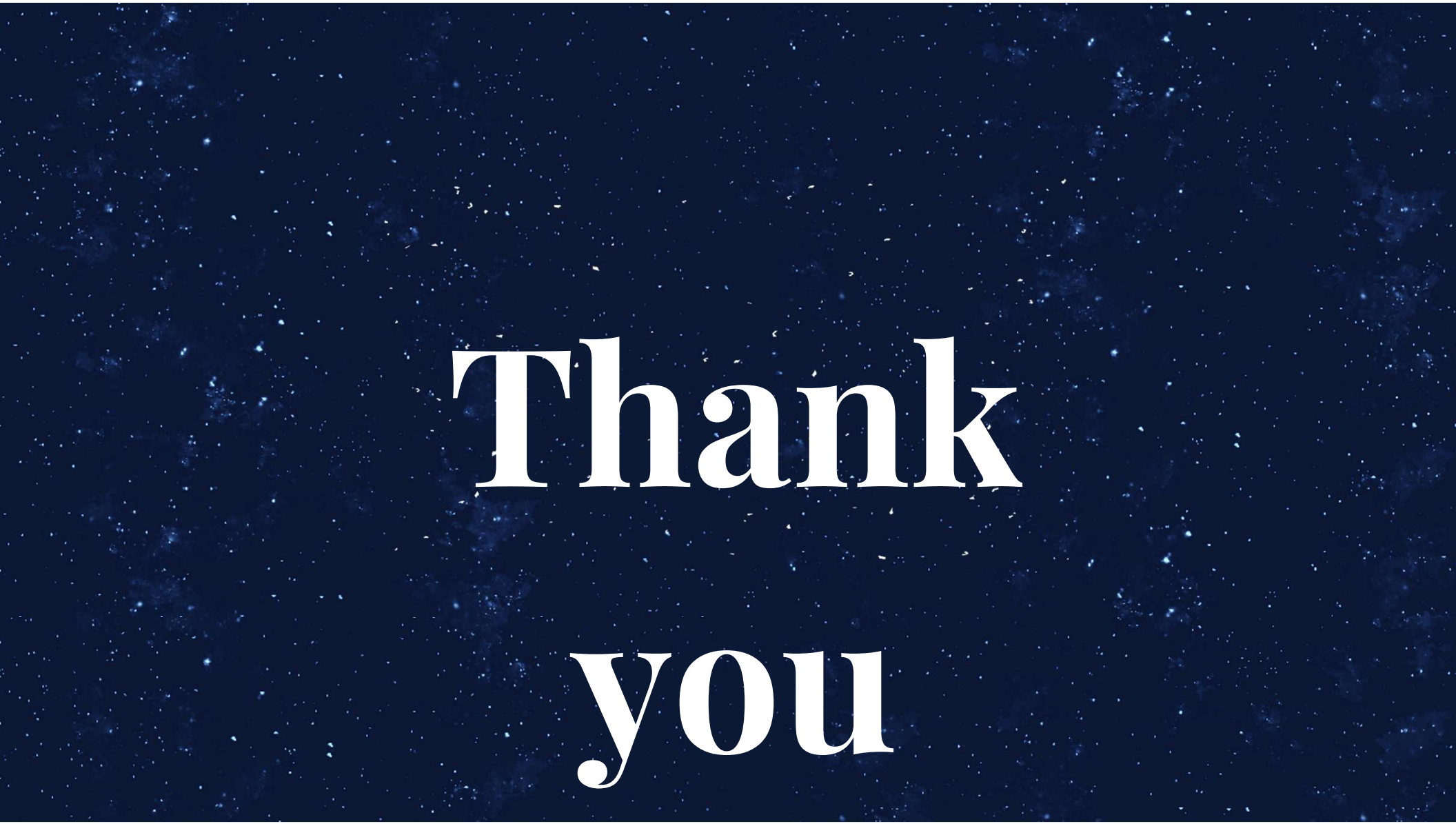
Additionally, as scam tactics continue to evolve, there's a risk of data drift, necessitating ongoing retraining of OCR systems to maintain their effectiveness. This continuous adaptation is crucial to ensure the technology remains reliable and accurate.

Moreover, when integrating OCR with Unified Payments Interface (UPI) platforms, compliance hurdles must be considered. This integration requires navigating regulatory approval processes to ensure that the technology adheres to legal and security standards. Addressing these challenges is vital for the successful deployment and operation of OCR systems in financial and security applications.

2_Bit_Army

Name of team members and their contact details:

SANGEETA PRASAD : +91 9110951296
SUJATA KUMARI : +91 80027 24946


Thank
you